НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«До захисту допущено»
Завідувач кафедри
_____ Леонід УРИВСЬКИЙ
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Аналіз ризиків в системах управління інформаційною безпекою»

Виконав:
студент ІІІ курсу, групи ТС-п71
Ісупов Павло Валентинович _____

Керівник:
Професор кафедри ТС, д.т.н., професор
Горицький Віктор Михайлович _____

Рецензент:

_____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Програма професійного спрямування (спеціалізація) – «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Леонід УРИВСЬКИЙ

«___»_____2020 р.

ЗАВДАННЯ

на дипломну роботу студенту

Ісупову Павлу Валентиновичу

1. Тема роботи «Аналіз ризиків в системах управління інформаційною безпекою», керівник роботи Горицький Віктор Михайлович, професор, д.т.н., затверджена наказом по університету від «30» березня 2020 р. № 924-с

2. Термін подання студентом роботи 12.06.2020

3. Вихідні дані: Розглянути систему технічного регулювання України, законодавства України у сфері технічного регулювання та підтвердження відповідності. Проаналізувати взаємозв’язок стандартів ISO/IEC 27000:2012, ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 27005:2011 та їх застосування. Дослідити процес управління ризиками інформаційної безпеки, ідентифікацію та визначення цінності активів, людські джерела загрози (хакер, крекер, комп'ютерний злочинець, індустріальне шпигунство тощо), вразливості і методи оцінки технічних вразливостей. Визначити сферу застосування та меж процесу системи управління інформаційною безпекою.

Примірний зміст текстової частини та терміни виконання за розділами.

1. Оцінка ризиків інформаційної безпеки – теоретичні засади 13.04.2020 –20.04.2020
2. Ризик-менеджмент відповідно до вимог стандарту ISO/IEC 27001:2013. 21.04.2020 – 2.05.2020
3. Аналіз та ідентифікація засобів управління інформаційною безпекою у системах і специфікаціях проектних вимог на стадії розробки 13.05.2020 –18.05.2020

Студент Павло ІСУПОВ

Керівник роботи Віктор ГОРИЦЬКИЙ

РЕФЕРАТ

Обсяг текстової частини дипломної роботи 55 сторінок. Кількість ілюстрацій 4,таблиць – 1, Кількість бібліографічних посилань 16.

Метою дипломної роботи є дослідження методів обробки ризиків та їх імплементацію у системах управління інформаційною безпекою відповідно до міжнародних стандартів.

Для досягнення поставленої мети в роботі вирішувалися наступні задачі:

а) розгляд ступеню відповідності системи управління інформаційною безпекою міжнародним стандартам;

б) аналіз сучасних систем фіксації та управління подіями інформаційної безпеки;

в) застосування підходів в оцінці ризиків інформаційної безпеки;

г) дослідження методів обробки ризиків у системах управління інформаційною безпекою.

Об’єкт дослідження – ризики у системах управління інформаційною безпекою.

Метод дослідження – аналітичний з використанням сучасної бази міжнародних стандартів та наукових досліджень за темою.

ABSTRACT

The volume of the text part of the thesis is 55 pages. Number of illustrations 4. Number of bibliographic references 16.

The purpose of the thesis is to study the methods of risk management and their implementation in information security management systems in accordance with international standards.

To achieve this goal, the following tasks were solved in the work:

a) consideration of the degree of compliance of the information security management system with international standards;

b) analysis of modern systems for recording and managing information security events;

c) application of approaches in assessing information security risks;

d) research of risk processing methods in information security management systems.

The object of research is risks in information security management systems.

The research method is analytical using a modern base of international standards and research on the topic.

ЗМІСТ

ВСТУП

Сучасні інформаційно-комунікаційні системи та мережі уразливі до ряду загроз, які можуть бути результатом реалізації несанкціонованого доступу, розкриття, викривлення або модифікації інформації, а також обмеження доступу до неї. Ці уразливості мають тенденції до посилення. Щоб захистити сучасні інформаційні ресурси та послуги від загроз, необхідно застосовувати відповідні заходи, засновані на комплексному підході до розробки та впровадження заходів та засобів захисту ресурсів інформаційно-комунікаційних систем та мереж як на технічному, так і на організаційному рівні. Зазначений процес забезпечує механізми та методи, які дозволяють реалізувати комплексну політику інформаційної безпеки організації. Інформаційна безпека – реалізація процесу захисту інформації від широкого діапазону загроз, що здійснюється з метою забезпечення ефективності та надійності функціонування інформаційно-комунікаційних систем та мереж.

Комплексний процес організації безпеки в першу чергу включає заходи управління інформаційною безпекою. Під управлінням інформаційною безпекою слід розуміти циклічний процес, що включає: постановку задачі захисту інформації; збір та аналіз даних про стан інформаційної безпеки в інформаційно-комунікаційних системах та мережах; оцінку інформаційних ризиків; планування заходів з обробки ризиків; реалізацію і впровадження відповідних механізмів контролю; розподіл ролей і відповідальності; політику безпеки; навчання та мотивацію персоналу, оперативну роботу по здійсненню захисних заходів; моніторинг (аудит) функціонування механізмів контролю, оцінку їх ефективності та надійності. Після ідентифікації вимог безпеки варто вибирати й застосовувати заходи управління таким чином, щоб забезпечувати впевненість у зменшені ризиків. Заходи управління сучасних інформаційно-комунікаційних систем та мереж включають [1]:

а) документи, що стосується політики інформаційної безпеки;

б) розподіл обов'язків, пов'язаних з інформаційною безпекою;

в) структура підрозділів й навчання, пов'язані з інформаційною безпекою;

г) повідомлення про інциденти, пов'язаних з безпекою;

д) управління безперервністю.

Засоби управління можуть бути обрані із стандартів або з безлічі інших документів та заходів управління визначених для даного класу систем, або можуть бути розроблені, щоб задовольнити потреби компанії відповідно до обраної політики безпеки.

Найбільш оптимальним рішенням на даний момент є необхідність застосування систем управління подіями інформаційної безпеки, зокрема - HP ArcSight. Це лінійка продуктів компанії Hewlett Packard, лідируючих у сфері моніторингу та контролю подій інформаційної безпеки. Рішення HP ArcSight здійснюють збір, обробку, зіставлення і реагування на такі події, надаючи всеосяжні функції масштабованості, захисту та відмовостійкості. Системи HP ArcSight дозволяє кожну хвилину обробляти сотні тисяч подій інформаційної безпеки, щоб автоматизувати рішення щодо забезпечення постійної інформаційної безпеки в організації.

Метою процесу управління ризиками інформаційної безпеки є виявлення, контроль та мінімізація невизначеності впливу чинників дестабілізації.

Для ефективного забезпечення інформаційної безпеки важливим є достатність різноманітних моделей та методів оцінки ризиків в системах управління інформаційною безпекою. Будь-яка оцінка ризиків інформаційної безпеки починається з обстеження інформаційної системи, ідентифікації інформаційних ресурсів та опису технологій обробки інформації.

При побудові систем управління інформаційною безпекою важливе місце займають процедури та процеси обробки ризиків на основі актуальних глобальних стандартів. Головним завданням стандартів безпеки є створення

основи для взаємодії між виробниками, споживачами та експертами з кваліфікації продуктів інформаційних технологій.

Можливі методи обробки ризиків [5]:

а) протидія ризикам - застосування належних заходів захисту;

б) свідоме та об'єктивне прийняття ризиків;

в) уникнення ризиків;

г) перенесення відповідних бізнес-ризиків на інші сторони, наприклад, страхувальників, постачальників.

Процес обробки ризиків включає в себе підготовку, вибір і прийняття рішень по способам обробки ризиків. Способи ці можуть бути самими різними. Головне, щоб вони були реалізовані й економічно виправдані. При інвестуванні грошей у зменшення ризику в результаті повинно виходити позитивне повернення інвестицій, яке являє собою різницю між витратами на безпеку і величиною запобігаємого збитку. Різниця ця повинна бути дуже істотною. Бажано, щоб повернення інвестицій перевищувало витрати на безпеку в рази.

На вхід цього процесу надходять результати оцінки ризиків у вигляді звіту і реєстр інформаційних ризиків, який додається до нього. Якщо ці дані є достатніми, тоді для кожної групи ризиків приймаються рішення по їх обробці шляхом вибору одного з чотирьох способів обробки ризиків або їх комбінації. При цьому використовуються критерії прийняття ризиків, які визначаються політикою організації в області управління ризиками. Результатом процесу обробки ризиків є план оброблення ризиків, що містить переліки заходів для кожної групи ризиків та оцінку остаточних ризиків.

Інструментом для успішного вирішення однієї з найскладніших завдань у впровадженні та розвитку систем управління інформаційною безпекою є оцінка та керівництво ризиками інформаційної безпеки на основі стандарту ISO/IEC 27005:2011 [7]. Цей підтримує загальні поняття, визначені у стандарті ISO/IEC 27001:2013, і призначений для забезпечення задовільної

реалізації інформаційної безпеки на основі підходу до управління ризиками, що є своєчасним та актуальним.

Метою обробки ризиків є їх зменшення до прийнятного рівня шляхом зменшення ймовірності інциденту або мінімізації можливих збитків.

Метою роботи є дослідження методів обробки ризиків та їх імплементацію у системах управління інформаційною безпекою відповідно до міжнародних стандартів.

Для досягнення поставленої мети в роботі вирішувалися наступні задачі:

д) розгляд ступеню відповідності системи управління інформаційною безпекою міжнародним стандартам;

е) аналіз сучасних систем фіксації та управління подіями інформаційної безпеки;

ж) застосування підходів в оцінці ризиків інформаційної безпеки;

з) дослідження методів обробки ризиків у системах управління інформаційною безпекою.

Об’єкт дослідження – ризики у системах управління інформаційною безпекою.

Метод дослідження – аналітичний з використанням сучасної бази міжнародних стандартів та наукових досліджень за темою.

1 ВІДПОВІДНІСТЬ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ МІЖНАРОДНИМ СТАНДАРТАМ

Сімейство міжнародних стандартів управління безпекою 27000 активно розвивається та призначене для забезпечення ІБ організації. Крім того, воно включає стандарти, що визначають вимоги до СУІБ, систему управління ризиками, метрики і вимірювання ефективності механізмів контролю, а також керівництво по впровадженню. Стандарти СУІБ включають стандарти, які: визначають вимоги до СУІБ, а також до тих, хто сертифікує такі системи; забезпечують безпосередню підтримку, містять докладні рекомендації і/або інтерпретацію загального процесу розробки, впровадження, забезпечення працездатності та поліпшення СУІБ; містять керівництва по СУІБ для конкретних галузей; містять вказівки з оцінки відповідності для СУІБ.

Міжнародна стандартизація в галузі ІБ охоплює стандарти, котрі умовно поділяються на 4 групи:

– стандарти для огляду і введення в термінологію;

– стандарти, які визначають обов’язкові вимоги до СУІБ (система управління інформаційною безпекою);

– стандарти, що визначають вимоги і рекомендації для аудиту СУІБ;

– стандарти, що пропонують кращі практики впровадження, розвитку та вдосконалення СУІБ.

Стандарти, які визначають обов’язкові вимоги до СУІБ, включають в себе ряд стандартів: ISO/IEC 27001 «Інформаційна технологія – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимоги», що зібрав описи найкращих світових практик в області управління інформаційною безпекою. Цей стандарт визначає вимоги до проектування, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою з урахуванням обставин організації, а також містить вимоги для оцінювання та оброблення ризиків інформаційної

безпеки, пов’язаних з потребами організації. Вимоги, наведені в ISO/IEC 27001, є загальними та можуть бути запроваджені для всіх організацій незалежно від типу, розміру та природи [6]. Крім того, документ встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Цей стандарт підготовлений як модель для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення системи менеджменту інформаційної безпеки [7].

1.1 Місце системи управління інформаційною безпекою в системі захисту інформації

Управління інформаційною безпекою - це циклічний процес, що включає: усвідомлення ступеня необхідності захисту інформації та постановку завдань, збір та аналіз даних про стан інформаційної безпеки в організації, оцінку інформаційних ризиків, планування заходів по обробці ризиків;, реалізацію та впровадження відповідних механізмів контролю, розподіл ролей і відповідальності, навчання і мотивацію персоналу, оперативну роботу по здійсненню захисних заходів; моніторинг функціонування механізмів контролю, оцінку їх ефективності та відповідні коригувальні дії.

Згідно ISO 27001, система управління інформаційною безпекою (СУІБ) - це частина загальної системи управління організації, заснованої на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки. Система управління включає в себе організаційну структуру, політики, планування, посадові обов'язки, практики, процедури, процеси і ресурси.

Створення та експлуатація СУІБ вимагає застосування такого ж підходу, як і будь-яка інша система управління. Використовувана в ISO

27001 для опису СУІБ процессная модель передбачає безперервний цикл заходів: планування; реалізація; перевірка; дія.

Процес безперервного вдосконалення зазвичай вимагає початкового інвестування: документування діяльності, формалізація підходу до управління ризиками, визначення методів аналізу і виділення ресурсів. Ці заходи застосовуються для приведення циклу в дію. Вони не обов'язково повинні бути завершені, перш ніж будуть активізовані стадії перегляду.

На стадії планування забезпечується правильне завдання контексту і масштабу СУІБ, оцінюються ризиків інформаційної безпеки, пропонується відповідний план обробки цих ризиків. У свою чергу, на стадії реалізації впроваджуються прийняті рішення, які були визначені на стадії планування. На стадіях перевірки і дії посилюють, виправляють і вдосконалюють Вашої оселі, які вже були визначені і реалізовані.

Перевірки можуть проводитися в будь-який час і з будь-якою періодичністю в залежності від конкретної ситуації. У деяких системах вони повинні бути вбудовані в автоматизовані процеси з метою забезпечення негайного виконання і реагування. Для інших процесів реагування потрібно тільки в разі інцидентів безпеки, коли в захищаються інформаційні ресурси були внесені зміни або доповнення, а також коли відбулися зміни загроз і вразливостей. Необхідні щорічні або інший періодичності перевірки або аудити, щоб гарантувати, що система управління в цілому досягає своїх цілей.

1.2 Аналіз стандартів системи управління інформаційною безпекою

Сімейство Міжнародних Стандартів на Системи Управління Інформаційною Безпекою 27000 розрорбляєтсья ISO/IEC JTC 1/SC 27. Це сімейство включає в себе Міжнародні стандарти, що визначають вимоги до системи управління інформаційної безпеки (СУІБ), управління ризиками, метрики і вимірювання, а також керівництво з впровадження.

Для цього сімейства стандартів використовується послідовна схема нумерації, починаючи з 27000.

Стандарт ISO/IEC 27001 описує загальну методологію підходу до забезпечення ІБ в організації і акцентує увагу на найбільш критичних складових ІС, Він охоплює елементи управління системою ІБ, актуальні для всіх сфер.

Цей стандарт дає компанії інструмент, що дозволяє управляти конфіденційністю, цілісністю і збереженням такого важливого активу компанії як інформація, Елементи управління системою ІБ розділені в стандарті по декількох груп, і включають в себе розділи

– Політика безпеки – підтримка політкики у сфері ІБ з боку керівництва підприємства;

– Інфраструктура системи безпеки – створення організаційної структури,яка буде забезпечувати працездатність системи ІБ;

– Класифікація ресурсів і управління – пріоритезація інформаційних ресурсів за ступенем їх цінності і розподіл відповідальності за них;

– Співробітники - зниження ризику людських помилок, крадіжки і неправильного використання устаткування,навчання співробітників та відстеження інцидентів;

– Фізична і зовнішня безпека - запобігання НСД та порушення роботи ІС організації;

– управління мережами і комп'ютерними ресурсами - забезпечення безпечного функціонування комп'ютерів та мереж;

– управління доступом - управління доступом до бізнес-інформації;

– відповідність вимогам законодавства - виконання вимог відповідного громадянського та кримінального законодавства, включаючи закони про авторські права і захист даних.

Стандарт складається з двох частин: в першій частині описані механізми контролю,(всього їх 127), необхідні для побудови СУІБ. Ця частина використовується в якості основи для проведення аудиту СУІБ в організації. У другій частині стандарту описуються ті критерії., по яких проводиться сертифікація СУІБ.

Виходячи з ідеології стандарту ключовим елементом СУІБ є система управління ризиками. Найважливішою частиною яких, є аналіз цих ризиків з метою визначення , які ресурси від яких загроз необхідно захищати, а також якою мірою ресурси потребують захисту.

Проведення аналізу ризиків дозволяє організації оцінити можливі збитки в кількісних і якісних показниках. Цей міжнародний стандарт був підготовлений для того, щоб надати модель для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримання в робочому стані і поліпшення СУІБ. Передбачається, що прийняття СУІБ є стратегічним для організації [3].

У відповідності з стандартом ISO/IEC 27001 документація, яка визначає управління інформаційними ризиками організації, повинна включати в себе:

- документовану заяву про політику та цілі СУІБ;
- область програми СУІБ;
- процедури і засоби управління на підтримку СУІБ;
- опис методології оцінки ризиків;
- звіт про оцінки ризиків;
- план обробки ризиків [3].

Міжнародний стандарт ISO / IEC 17799: 2000 (BS 7799-1: 2000) «Управління інформаційною безпекою - Інформаційні технології»

(«Information technology - Information security management) є одним з найбільш відомих стандартів в області захисту інформації. Даний стандарт був розроблений на основі першої частини Британської стандарту BS 7799-1: +1995 «Практичні рекомендації з управління інформаційною безпекою» (

«lnformation security management - Part 1: Code of practice for information security management) і відноситься до нового покоління стандартів інформаційної безпеки комп'ютерних ІС.

Поточна версія стандарту ISO / IEC 17799: 2000 (BS 7799-1: 2000) розглядає такі актуальні питання забезпечення інформаційної безпеки організацій та підприємств:

– необхідність забезпечення інформаційної безпеки;
– основні поняття і визначення інформаційної безпеки;
– політика інформаційної безпеки компанії;
– організація інформаційної безпеки на підприємстві;
– класифікація та управління корпоративними інформаційними ресурсами;
– кадровий менеджмент та інформаційна безпека;
– фізична безпека;
– адміністрування безпеки КІС;
– управління доступом;
– вимоги щодо безпеки до КІС в ході їх розробки, експлуатації і супроводу;
– управління бізнес-процесами компанії з точки зору інформаційної безпеки;
– внутрішній аудит інформаційної безпеки компанії.

Друга частина стандарту BS 7799-2 2000 «Специфікації систем управління інформаційною безпекою» («Information security management - Part 2: Specification for information security management systems»), визначає можливі функціональні специфікації корпоративних систем управління інформаційною безпекою з точки зору їх перевірки на відповідність вимогам першої частини даного стандарту. Відповідно до положень цього стандарту також регламентується процедура аудиту КІС.

Додаткові рекомендації для управління інформаційною безпекою містять керівництва Британського інституту стандартів - British Standards Institution (BSI), видані в 1995-2003 рр. у вигляді такої серії:

– «Введення в проблему управління інформаційною безпекою» («Information security managment: an introduction);

– «Можливості сертифікації на вимоги стандарту BS 7799» («Preparing for BS 7799 sertification»);

– «Керівництво BS 7799 з оцінки та управління ризиками» («Guide to BS 7799 risk assessment and risk management);

– «Керівництво для проведення аудиту на вимоги стандарту» («BS 7799 Guide to BS 7799 auditing);

– «Практичні рекомендації з управління безпекою інформаційних технологій» («Code of practice for IT management).

У 2002 р міжнародний стандарт ISO 17799 (BS 7799) був переглянутий і суттєво доповнено. У новому варіанті цього стандарту велику увагу приділено питанням підвищення культури захисту інформації в різних міжнародних компаніях. На думку фахівців, оновлення міжнародного стандарту ISO 17799 (BS 7799) дозволить не тільки підвищити культуру захисту інформаційних активів компанії, але і скоординувати дії різних провідних державних і комерційних структур в області захисту інформації.

На відміну від ISO 17799 німецьке «Керівництво щодо захисту інформаційних технологій для базового рівня захищеності» присвячено детальному розгляду приватних питань управління інформаційною безпекою компанії.

У німецькому стандарті BSI представлені:

– загальна методика управління інформаційною безпекою (організація менеджменту в області інформаційної безпеки, методологія використання керівництва);

– опису компонентів сучасних IT;

– опису основних компонентів організації режиму інформаційної безпеки (організаційний і технічний рівні захисту даних, планування дій у надзвичайних ситуаціях, підтримка безперервності бізнесу);

– характеристики об'єктів інформатизації (будівлі, приміщення, кабельні мережі, контрольовані зони);

– характеристики основних інформаційних активів компанії (в тому числі апаратне і програмне забезпечення, наприклад робочі станції і сервери під управлінням ОС сімейства DOS, Windows і UNIX);

– характеристики комп'ютерних мереж на основі різних мережевих технологій, наприклад мережі Novell NetWare, мережі UNIX і Windows).

– характеристика активного і пасивного телекомунікаційного обладнання провідних постачальників, наприклад Cisco Systems;

– докладні каталоги загроз безпеки і заходів контролю (більше 600 найменувань в кожному каталозі).

Питання захисту наведених інформаційних активів компанії розглядаються за певним сценарієм: загальний опис інформаційного активу компанії - можливі загрози і вразливості безпеки - можливих заходів, і засоби контролю та захисту.

Міжнародний стандарт ISO 15408 «Загальні критерії безпеки інформаційних технологій»

Одним з головних результатів стандартизації у сфері систематизації вимог і характеристик захищених інформаційних комплексів стала система міжнародних і національних стандартів безпеки інформації, яка налічує більше сотні різних документів. Важливе місце в цій системі стандартів займає стандарт ISO 15408, відомий як «Common Criteria for Information Technology Security Evaluation».

У 1990 р Міжнародна організація по стандартизації (ISO) приступила до розробки міжнародного стандарту із критеріями оцінки безпеки IT для загального використання. У розробці брали участь: Національний інститут стандартів і технології і Агентство національної безпеки (США), Установа

безпеки комунікацій (Канада), Агентство інформаційної безпеки (Німеччина), Агентство національної безпеки комунікацій (Голландія), органи виконання Програми безпеки і сертифікації ІТ (Англія), центр забезпечення безпеки систем (Франція), які спиралися на свій солідний заділ.

За десятиліття розробки кращими фахівцями світу документ неодноразово редагувався. Перші дві версії були опубліковані відповідно в січні і травні 1998 р Версія 2.1 цього стандарту затверджена 8 червня 1999 р Міжнародною організацією зі стандартизації (ISO) в якості міжнародного стандарту інформаційної безпеки ISO / IEC 15408 під назвою «Загальні критерії оцінки безпеки інформаційних технологій» , або «Common Criteria».

«Загальні критерії» (ЗК) узагальнили зміст і досвід використання Помаранчевої книги, розвинули європейські та канадські критерії і втілили в реальні структури концепцію типових профілів захисту федеральних критеріїв США.

В ЗК проведена класифікація широкого набору вимог безпеки ІТ, визначені структури їх групування і принципи використання. Головні переваги ЗК - повнота вимог безпеки і їх систематизація, гнучкість в застосуванні і відкритість для подальшого розвитку.

Провідні світові виробники обладнання ІТ відразу стали поставляти замовникам кошти, які повністю відповідають вимогам ЗК.

ЗК розроблялися для задоволення запитів трьох груп фахівців, в рівній мірі є користувачами цього документа: виробників і споживачів продуктів ІТ, а також експертів з оцінки рівня їх безпеки. ЗК забезпечують нормативну підтримку процесу вибору ІТ-продукту, до якого пред'являються вимоги функціонування в умовах дії певних загроз, служать керівним матеріалом для розробників таких систем, а також регламентують технологію їх створення та процедуру оцінки забезпечується рівня безпеки.

ЗК розглядають інформаційну безпеку, по-перше, як сукупність конфіденційності і цілісності інформації, що обробляється ІТ-продуктом, а також доступності ресурсів ВС і, по-друге, ставлять перед засобами захисту

завдання протидії загрозам, актуальним для середовища експлуатації цього продукту і реалізації політики безпеки , прийнятої в цьому середовищі експлуатації. Тому в концепцію ЗК входять всі аспекти процесу проектування, виробництва і експлуатації ІТ-продуктів, призначених для роботи в умовах дії певних загроз безпеки.

Споживачі ІТ-продуктів стурбовані наявністю загроз безпеки, що призводять до певних ризиків для оброблюваної інформації. Для протидії цим загрозам ІТ-продукти повинні включати в свій склад засоби захисту, які протидіють цим загрозам і спрямовані на усунення вразливостей, проте помилки в засобах захисту в свою чергу можуть призводити до появи нових вразливостей. Сертифікація засобів захисту дозволяє підтвердити їх адекватність загрозам і ризикам.

ЗК регламентують всі стадії розробки, кваліфікаційного аналізу та експлуатації ІТ-продуктів. ЗК пропонують концепцію процесу розробки і кваліфікаційного аналізу ІТ-продуктів, що вимагає від споживачів і виробників великої роботи зі складання та оформлення об'ємних і докладних нормативних документів.

Вимоги ЗК є практично всеосяжної енциклопедією інформаційної безпеки, тому їх можна використовувати в якості довідника з безпеки ІТ.

Стандарт ISO 15408 підняв стандартизацію ІТ на міждержавний рівень. Виникла реальна перспектива створення єдиного безпечного інформаційного простору, в якому сертифікація безпеки систем обробки інформації буде здійснюватися на глобальному рівні, що надасть можливості для інтеграції національних ІС, що в свою чергу відкриє нові сфери застосування ІТ.

У 1990 році Комітет IEEE 802 сформував робочу групу 802.11 для розробки стандарту для бездротових локальних мереж. Роботи зі створення стандарту були завершені через 7 років. У 1997 р була ратифікована перша специфікація бездротового стандарту IEEE 802.11, що забезпечує передачу даних з гарантованою швидкістю 1 Мб / с (в деяких випадках до 2 Мб / с) в

смузі частот 2,4 ГГц. Ця смуга частот доступна для неліцензійного використання в більшості країн світу.

Стандарт IEEE 802.11 є базовим стандартом і визначає протоколи, необхідні для організації бездротових локальних мереж WLAN (Wireless Local Area Network). Основні з них - протокол управління доступом до середовища MAC (Medium Accsess Control - нижній підрівень канального рівня) і протокол PHY передачі сигналів у фізичному середовищі. Як фізичне середовище допускається використання радіохвиль і інфрачервоних променів.

В основу стандарту IEEE 802.11 покладена стільникова архітектура, причому мережа може складатися як з однієї, так і декількох осередків. Кожна з них управляється базовою станцією, званою точкою доступу AP (Access Point), яка разом з розташованими в межах радіусу її дії робочими станціями користувачів утворює базову зону обслуговування BSS (Basic Service Set). Точки доступу багатостільникової мережі взаємодіють між собою через розподільну систему DS (Distribution System), що є еквівалентом магістрального сегменту кабельних ЛС. Вся інфраструктура, що включає точки доступу і розподільну систему утворює розширену зону обслуговування ESS (Extended Service Set). Стандартом передбачений також односотовий варіант бездротової мережі, який може бути реалізований і без точки доступу, при цьому частина її функцій виконуються безпосередньо робочими станціями.

Для забезпечення переходу мобільних робочих станцій із зони дії однієї точки доступу до іншої в многосотовую системах передбачені спеціальні процедури сканування (активного і пасивного прослуховування ефіру) і приєднання (Association), однак строгих специфікацій по реалізації роумінгу стандарт IEEE 802.11 не передбачає.

Для захисту WLAN стандартом IEEE 802.11 передбачено алгоритм WEP (Wired Equivalent Privacy). Він включає засоби протидії

несанкціонованого доступу до мережі, а також шифрування для запобігання перехоплення інформації.

Однак закладена в першу специфікацію стандарту IEEE 802.1 1 швидкість передачі даних в бездротовій мережі перестала задовольняти потребам користувачів: алгоритм WEP мав ряд істотних недоліків - відсутність управління ключем, використання загального статичного ключа, малі розрядності ключа і вектора ініціалізації, складності використання алгоритму RC4.

Щоб зробити технологію Wireless LAN недорогою, популярною і задовольнити жорстким вимогам бізнес-додатків, розробники створили сімейство нових специфікацій стандарту IEEE 802.11 - a, b, l Стандарти цього сімейства, по суті, є бездротовими розширеннями протоколу Ethernet, що забезпечує хорошу взаємодію з провідними мережами Ethernet.

Стандарт IEEE 802.11b був ратифікований IEEE у вересні 1999 р. як розвиток базового стандарту 802.11; в ньому використовується смуга частот 2,4 ГГц, швидкість передачі досягає 11 Мб / с (подібно Ethernet). Завдяки орієнтації на освоєний діапазон 2,4 ГГц стандарт 802.11b завоював велику популярність у виробників устаткування. В якості базової радіотехнології в ньому використовується метод розподіленого спектра з прямою послідовністю DSSS (Direct Sequence Spread Spectrum), який відрізняється високою стійкістю до спотворення даних перешкодами, в тому числі навмисними. Цей стандарт набув широкого поширення, і бездротові LAN стали привабливим рішенням з технічної та фінансової точки зору.

Стандарт IEEE 802.11a призначений для роботи в частотному діапазоні 5 ГГц. Швидкість передачі даних до 54 Мбіт / с, т. Е. Приблизно в 5 разів швидше мереж 802.1 lb. Асоціація WECA називає цей стандарт Wi-Fi5. Це найбільш широкосмуговий стандарт з сімейства стандартів 802.11. Визначено три обов'язкові швидкості - 6, 12 і 24 Мбіт / с і п'ять необов'язкових - 9, 18, 36, 48 і 54 Мбіт / с. В якості методу модуляції сигналу прийнято ортогональное частотне мультиплексування OFDM (Orthogonal

Frequency Division Multiplexing). Його відмінність від методу DSSS полягає в тому, що OFDM передбачає паралельну передачу корисного сигналу одночасно за кількома частотам діапазону, в той час як технології розширення спектру DSSS передають сигнали послідовно. В результаті підвищується пропускна здатність каналу і якість сигналу. До недоліків стандарту 802.11a відноситься велика споживана потужність радіопередавачів для частот 5 ГГц, а також менший радіус дії (близько 100 м). Для простоти запам'ятовування в якості загального імені для стандартів 802.1 lb і 802.11a, а також всіх подальших, що відносяться до бездротових локальних мереж (WLAN), Асоціацією бездротової сумісності з Ethernet WECA (Wireless Ethernet Compatibility Aliance) був введений термін Wi-Fi (Wireless Fidelity). Якщо пристрій позначено цим знаком, воно протестовано на сумісність з іншими пристроями 802.11.

Стандарт IEEE 802.1 lg є розвиток 802.11b і назад сумісний з 802.11b; призначений для забезпечення швидкостей передачі даних до 54 Мбіт / с. У числі переваг 802.1 Ig треба відзначити низьку споживану потужність, великі відстані (до 300 м) і високу проникаючу здатність сигналу.

Стандарт IEEE 802.1 li - стандарт забезпечення безпеки в бездротових мережах; ратифікований IEEE в 2004 р Цей стандарт вирішив існували проблеми в області аутентифікації і протоколу шифрування, забезпечивши значно вищий рівень безпеки. Стандарт 802.11 і може застосовуватися в мережах Wi-Fi, незалежно від використовуваного стандарту - 802.1l a, b або g.

Існують два дуже схожих стандарту - WPA і 802.1 П. WPA був розроблений в Wi-Fi Alliance як рішення, яке можна застосувати негайно, не чекаючи завершення тривалої процедури ратифікації 802.1 li в IEEE. Обидва стандарти використовують механізм 802.1x для забезпечення надійної аутентифікації, обидва використовують сильні алгоритми шифрування і призначені для заміни протоколу WEP.

Їх основна відмінність полягає в використанні різних механізмів шифрування. В WPA застосовується протокол TKIP (Temporal Key Integrity Protocol), який, також як і WEP, використовує шифр RC4, але значно більш безпечним способом. Забезпечення конфіденційності даних в стандарті IEEE 802.1 li засноване на використанні алгоритму шифрування AES (Advanced Encryption Standard). Використовує його захисний протокол отримав назву Ccmp (Counter-Mode CBC MAC Protocol). Алгоритм AES володіє високою криптостійкості-стю. Довжина ключа AES дорівнює 128, 192 або 256 біт, що забезпечує найбільш надійне шифрування з доступних зараз.

Стандарт 802.1 передбачає наявність трьох учасників процесу аутентифікації. Це сервер аутентифікації AS (Authentication Server), точка доступу AP (Access Point) і робоча станція STA (Station). У процесі шифрування даних беруть участь тільки AP і STA (AS не використовується). Стандарт передбачає двосторонню аутентифікацію (на відміну від WEP, де ау-тентіфіціруется тільки робоча станція, але не точка доступу). При цьому місцями прийняття рішення про дозвіл доступу є сервер аутентифікації AS і робоча станція STA, а місцями виконання цього рішення - точка доступу AP і STA.

Для роботи за стандартом 802.1 li створюється ієрархія ключів, що містить майстер-ключ МК (Master Key), парний майстер-ключ РМК (Pairwise Master Key), парний тимчасовий ключ РТК (Pairwise Transient Key), а також групові тимчасові ключі GTK (Group Transient Key), службовці для захисту широковещательного мережевого трафіку.

МК - це симетричний ключ, який реалізує рішення STA і AS про взаємну аутентифікації. Для кожної сесії створюється новий МК.

РМК - оновлюваний симетричний ключ, володіння яким означає дозвіл (авторизацію) на доступ до середовища передачі даних протягом даної сесії. РМК створюється на основі МК. Для кожної пари STA і AP у кожної сесії створюється новий РМК.

РТК - це колекція операційних ключів, які використовуються для прив'язки РМК до даних STA і AP, поширення GTK і шифрування даних.

Процес аутентифікації і доставки ключів визначається стандартом 802.1 x. Він надає можливість використовувати в бездротових мережах такі традиційні сервери аутентифікації, як RADIUS (Remote Authentication Dial-In User Server). Стандарт 802.1 li не визначає тип сервера аутентифікації, але використання RADIUS для цієї мети є стандартним рішенням.

Транспортом для повідомлень 802.1x служить протокол EAP (Extensible Authentication Protocol). EAP дозволяє легко додавати нові методи аутентифікації. Точки доступу не потрібно знати про використаний метод аутентифікації, тому зміна методу ніяк не зачіпає точку доступу. Найбільш популярні методи EAP - це LEAP, PEAP, TTLS і FAST. Кожен з методів має свої сильні і слабкі сторони, умови застосування, по-різному підтримується виробниками обладнання і ПЗ. Виділяють п'ять фаз роботи 802.1 П.

Перша фаза - виявлення. У цій фазі робоча станція STA знаходить точку доступу AP, з якої може встановити зв'язок і отримує від неї використовуються в даній мережі параметри безпеки. Таким чином STA дізнається ідентифікатор мережі SSID і методи аутентифікації, доступні в даній мережі. Потім STA вибирає метод аутентифікації, і між STA і AP встановлюється з'єднання. Після цього STA і AP готові до початку другої фази 802.1x.

Друга фаза - аутентифікація. У цій фазі виконується взаємна аутентифікація STA і сервера AS, створюються МК і РМК. У цій фазі STA і AP блокують весь трафік, крім трафіку 802.1x.

Третя фаза - AS переміщує ключ РМК на AP. Тепер STA і AP володіють дійсними ключами РМК.

Четверта фаза - управління ключами 802.1x. У цій фазі відбувається генерація, прив'язка і верифікація ключа РТК.

П'ята фаза - шифрування і передача даних. Для шифрування використовується відповідна частина РТК.

Стандартом 802.1 li передбачений режим PSK (Pre-Shared Key), який дозволяє обійтися без сервера аутентифікації AS. При використанні цього режиму на STA і на AP вручну вводиться Pre-Shared Key, який використовується в якості РМК. Далі генерація РТК відбувається описаним вище порядком. Режим PSK може використовуватися в невеликих мережах, де недоцільно встановлювати AS.

В Інтернеті популярні протоколи передачі даних SSL, SET, IPSec. Перераховані протоколи з'явилися в Інтернеті в середині 90-х років XX століття,оскільки необхідність захисту цінної інформації з часом значно зросла.

Протокол SSL (Secure Socket Layer) - популярний мережевий протокол з шифруванням даних для безпечної передачі по мережі. Він дозволяє встановлювати захищене з'єднання, проводити контроль цілісності даних і вирішувати різні супутні завдання. Протокол SSL забезпечує захист даних між сервісними протоколами (такими як HTTP, FTP та ін.) і транспортними протоколами (TCP / IP) за допомогою сучасної криптографії.

Протокол SET (Security Electronics Transaction) - перспективний стандарт безпечних електронних транзакцій в мережі Інтернет, призначений для організації електронної торгівлі через мережу Інтернет. Протокол SET заснований на використанні цифрових сертифікатів за стандартом X.509.

Протокол виконання захищених транзакцій SET є стандартом, розробленим компаніями MasterCard і Visa при значній участі IBM, GlobeSet та інших партнерів. Він дозволяє покупцям купувати товари через Інтернет, використовуючи захищений механізм виконання платежів.

SET є відкритим стандартним багатостороннім протоколом для проведення безпечних платежів з використанням пластикових карток в Інтернеті. SET забезпечує крос-аутентифікацію рахунку власника картки, продавця і банку продавця для перевірки готовності оплати, а також цілісність і секретність повідомлення, шифрування цінних та вразливих даних. Тому SET більш правильно можна назвати стандартною технологією

або системою протоколів виконання безпечних платежів з використанням пластикових карт через Інтернет. SET дозволяє споживачам і продавцям підтверджувати справжність всіх учасників угоди, яка відбувається в Інтернеті, за допомогою криптографії, в тому числі застосовуючи цифрові сертифікати.

Як згадувалося раніше, базовими завданнями захисту інформації є забезпечення її доступності, конфіденційності, цілісності та юридичної значимості. SET, на відміну від інших протоколів, дозволяє вирішувати зазначені завдання захисту інформації в цілому.

Зокрема, він забезпечує наступні спеціальні вимоги захисту операцій електронної комерції:

– таємність даних оплати і конфіденційність інформації замовлення, переданої поряд з даними про оплату;

– збереження цілісності даних платежів. Цілісність інформації платежів забезпечується за допомогою цифрового підпису;

– спеціальну криптографію з відкритим ключем для проведення аутентифікації;

– аутентифікацію по кредитній картці. Вона забезпечується застосуванням цифрового підпису та сертифікатів власника карт;

– аутентифікацію продавця і його можливості приймати платежі за пластиковими картками із застосуванням цифрового підпису та сертифікатів продавця;

– аутентифікацію того, що банк продавця є діючою організацією, яка може приймати платежі за пластиковими картками через зв'язок з процессинговой картковою системою. Аутентифікація банку продавця забезпечується використанням цифрового підпису і сертифікатів банку продавця;

– готовність оплати транзакцій в результаті аутентифікації сертифіката з відкритим ключем для всіх сторін;

– безпеку передачі даних за допомогою переважного використання криптографії.

Основна перевага SET в порівнянні з іншими існуючими системами забезпечення інформаційної безпеки полягає в використанні цифрових сертифікатів (стандарт X509, версія 3), які асоціюють власника картки, продавця і банк продавця з банківськими установами платіжних систем Visa і Mastercard. Крім того, SET дозволяє зберегти існуючі відносини між банком, власниками карт і продавцями і інтегрується з існуючими системами.

Протокол IPSec. Специфікація IPSec входить в стандарт IP v.6 і є додатковою по відношенню до поточної версії протоколів TCP / IP. Вона розроблена Робочою групою IP Security IETF. В даний час IPSec включає 3 Алгоритм-неза-мих базових специфікації, що представляють відповідні RFC-стандарти. Протокол IPSec забезпечує стандартний спосіб шифрування трафіку на мережевому (третьому) рівні IP і захищає інформацію на основі наскрізного шифрування: незалежно від ефектів у програмному забезпеченні при цьому шифрується кожен пакет даних, що проходить по каналу. Це дозволяє організаціям створювати в Інтернеті віртуальні приватні мережі.

Інфраструктура управління відкритими ключами PKI (Public Key Infrastructure) призначена для захищеного управління криптографічними ключами електронного документообігу, заснованого на застосуванні криптографії з відкритими ключами. Ця інфраструктура має на увазі використання цифрових сертифікатів, які відповідають рекомендаціям міжнародного стандарту X.509 і розгорнутої мережі центрів сертифікації, що забезпечують видачу та супровід цифрових сертифікатів для всіх учасників електронного обміну документами.

1.3 Система управління інформаційною безпекою та вигоди сертифікації

Система управління інформаційною безпекою (Information Security Management System, ISMS) – це частина загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводження та вдосконалення заходів у галузі інформаційної безпеки. Цю систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Найбільш значущою метою більшості систем інформаційної безпеки є захист бізнесу та знань компанії від знищення або витоку. Також однією з основних цілей системи інформаційної безпеки є гарантія майнових прав та інтересів клієнтів. У той же час заходи з інформаційної безпеки не повинні обмежувати або ускладнювати процеси обміну інформацією в компанії, оскільки це може поставити під загрозу розвиток організації.

Система управління інформаційною безпекою повинна забезпечувати гарантію досягнення таких цілей як забезпечення конфіденційності критичної інформації, забезпечення неможливості несанкціонованого доступу до критичної інформації, цілісності інформації та пов'язаних з нею процесів (створення, введення, обробки і виведення) і ряду інших цілей.

Досягнення заданих цілей можливо у ході вирішення таких основних завдань, як визначення відповідальних за інформаційну безпеку, розробка спектра ризиків інформаційної безпеки та проведення їх експертних оцінок, розробка політик і правил доступу до інформаційних ресурсів, розробка системи управління ризиками інформаційної безпеки, у тому числі методи їх оцінки, контролю інформаційної безпеки на підприємстві. Слід зазначити, що тут перераховано не повний список.

Побудова СУІБ дозволяє чітко визначити, як взаємопов'язані процеси та підсистеми ІБ, хто за них відповідає, які фінансові та трудові ресурси необхідні для їх ефективного функціонування, і т.д.

Основні функції системи управління інформаційною безпекою:

– виявлення та аналіз ризиків інформаційної безпеки;

– планування та практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ;

– контроль цих процесів;

– внесення в процеси мінімізації інформаційних ризиків необхідних коригувань.

Якісне управління інформаційною безпекою базується на наступних принципах:

– комплексний підхід – управління ІБ має бути всеосяжним, охоплювати всі компоненти ІС і враховувати всі актуальні ризикоутворюючі фактори, що діють в інформаційній системі підприємства та за її межами;

– узгодженість з бізнес-задачами і стратегією підприємства;

– високий рівень керованості;

– адекватність інформації, яка використовується і генерується;

– ефективність – оптимальний баланс між можливостями, продуктивністю і витратами СУІБ;

– безперервність управління;

– процесний підхід – зв’язування процесів управління в замкнутий цикл планування, впровадження, перевірки, аудиту та коригування, і підтримка нерозривного зв’язку між етапами.

Одним з ключових чинників успішності системи управління інформаційною безпекою підприємства – це побудова її на базі міжнародних стандартів ISO 27001 .Міжнародний стандарт ISO 27001 надає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої системи управління інформаційною безпекою в контексті розгляду бізнес ризиків.

Переваги сертифікації ISO / IEC 27001 для вашої організації:

– Забезпечує ефективну основу для вищого керівництва;

– Надає вам конкурентну перевагу;

– Зниження витрат, пов'язаних з інцидентами, і мінімізація загроз;

– Можливість продемонструвати відповідність вимогам клієнтів, нормативним та іншим вимогам;

– Визначає сфери відповідальності в рамках всієї організації;

– Дає позитивний посил для співробітників, клієнтів, постачальників і зацікавлених сторін;

– Узгодженість між бізнес-операціями і інформаційною безпекою;

– Узгодження інформаційної безпеки з цілями організації.

Для ваших клієнтів:

– Гарантія захищеності інтелектуальної власності та цінної інформації;

– Впевненість клієнтів і зацікавлених сторін в правильному управлінні ризиками;

– Безпечний обмін інформацією;

– Гарантія відповідності юридичним зобов'язанням;

– Мінімізація схильності до ризику;

– Економія витрат на виправлення помилок.

1.4 Висновки до розділу 1

Системи управління інформаційною безпекою ISMS застосовують у всіх типах організацій та у всіх видів підприємницької діяльності, навіть для малих та середніх підприємств (SMEs), які виконують функцію ланцюгів постачання, через це дуже важливо, щоб вони контролювали та керували своєю інформаційною безпекою та кібер-ризиками, щоб захистити себе та інших.

2 АНАЛІЗ СУЧАСНИХ СИСТЕМ ФІКСАЦІЇ ТА УПРАВЛІННЯ ПОДІЯМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розвиток інформаційних технологій спрощує ведення бізнесу. Однак, чим більше джерел даних з'являється в корпоративних IT-системах, тим складніше стають завдання адміністраторів інформаційної безпеки, які не встигають «вручну» відстежувати і блокувати загрози. Без своєчасного моніторингу та запобігання несанкціонованих дій втрачається сенс системи захисту інформації. І тут на допомогу ІБ-фахівцям приходять рішення класу SIEM - Security Information and Event Management.

Сучасні кіберзлочинці не атакують безпосередньо IT-інфрастуктуру. Вони діють завуальовано, використовуючи вразливості захисних ресурсів. Такі інциденти залишаються поза увагою, так як без «контексту» не вказують на загрозу. Відстежити протиправні дії допомагає постійний моніторинг і аналіз всіх подій, що відбуваються в IT-інфраструктурі компанії. Таку здатність аналізувати і виявляти інциденти по окремим подіям мають SIEM-рішення.

Згідно з дослідженням Garther, в число лідерів в 2018 році увійшли наступні системи: Splunk, IBM і LogRhythm [11]. Наведемо їх коротку характеристику:

Компанія IBM пропонує комплексне рішення в області SIEM-систем, яке називається Tivoli Security Information and Event Manager (TSIEM). TSIEM дозволяє, з одного боку, проводити аудит подій безпеки на відповідність внутрішнім політикам і різним міжнародним стандартам, а з іншого боку - здійснювати обробку інцидентів, пов'язаних з інформаційною безпекою, і виявляти атаки та інші загрози для елементів інфраструктури. В області подання та зберігання подій TSIEM використовує запатентовану методику W7 (Who, did What, When, Where, Wherefrom, Where to and on What), відповідно до якої всі події трансформуються в єдиний формат, зрозумілий адміністраторам безпеки, аудиторам і управлінцям. Також TSIEM

володіє розвиненими можливостями щодо формування звітів і моніторингу активності користувачів.

Splunk - це ще одне рішення для ведення комерційних журналів подій, яке позиціонується як рішення «Пошук в IT» і вбудовується в такі продукти, як Cisco System IronPort. Завдяки веб-інтерфейсу Splunk інтуїтивно зрозумілий в налаштуванні і управлінні. Splunk використовує досить зручний для користувача підхід до проектування інтерфейсів, спрощуючи початковий досвід для менш досвідченого адміністратора. Як і у багатьох аналогічних продуктів для ведення журналів, можливість створення звітів є частиною базового продукту і, в разі Splunk, вона відносно проста у використанні. Поширені типи форматів представлення даних доступні з розкривних меню на екрані. Одна з приємних сторін веб-інтерфейсу Splunk полягає в тому, що будь-який звіт може бути наданий у вигляді URL-адреси, що дозволяє іншим людям в організації переглядати конкретні звіти, які системний адміністратор створює для них.

LogRhythm, Inc. - американська компанія, що займається питаннями безпеки, яка об'єднує систему управління інформацією і подіями безпеки (SIEM), управління журналами, моніторинг мережі і кінцевих точок, а також аналітику і безпеку. LogRhythm стверджує, що допомагає клієнтам швидко виявляти і реагувати на кіберзагрози, перш ніж буде завдано істотної шкоди. Він також націлений на забезпечення автоматизації та відповідності нормативним вимогам. Продукти LogRhythm покликані допомогти організаціям захистити свої мережі і оптимізувати роботу. Крім того, вони допомагають автоматизувати збір, організацію, аналіз, архівування та відновлення даних журналів, що дозволяє компаніям дотримуватися правил зберігання даних журналів. Компоненти продукту включають в себе збір даних, моніторинг системи і мережі, аналітичні модулі, управління журналами і подіями.

Останнім часом на ринку з'являються вітчизняні рішення, серед яких:

KOMRAD Enterprise SIEM - здатна здійснювати єдиний контроль подій інформаційної безпеки, виявляти виникаючі інциденти інформаційної безпеки, оперативно реагувати на що з'являються загрози, відповідати вимогам що ставляться до захисту особистої інформації, здатний забезпечувати збереження державних інформаційних систем. Перевагами використання даної системи можна вважати: підтримку великої кількості платформ, своєчасне інформування та реагування на різні види загроз, можливість гнучкого налаштування, віддалене управління конфігураціями, збір інформації з нестандартних джерел подій.

Security Capsule - перша Російська система контролю за інформаційною безпекою. Є найбільш доступною серед застосовуваних у Росії SIEM - систем. Володіє такими якостями: виявлення мережевих атак як в локальних, так і в глобальних периметрах, виявлення вірусних заражень, здатність реєструвати події в використовуваною операційною системою, облік дій осіб, які взаємодіють з системою управління базою даних.

MaxPatrol SIEM - система, що має об'єктивну оцінку рівня захищеності як окремо взятих підрозділів, вузлів і додатків, так і всієї системи в цілому. У порівнянні з вище розглянутим програмним продуктом виділяється більш високою вартістю. Дана система характеризується використанням евристичних механізмів аналізу та сформованої базою знань, здатної здійснювати перевірку більшості поширених операційних систем і спеціалізованої апаратури. На відміну від класичних SIEM-систем, вона не потребує встановлення програмних компонентів на вузлах, що істотно полегшує процес використання і знижує кінцеву вартість володіння. Володіє легко настроюється системою і розмежуванням прав доступу, що дає можливість формувати моніторинг ІБ на кожному з рівнів ієрархії. Для окремо взятого користувача MaxPatrol, присутня можливість створити свій список завдань, які він здатний виконати всередині системи.

RUSIEM - система розроблена компанією ТОВ «АйТі Таск». За задумом розробників, продукт повинен замінити зарубіжні аналоги на

російському ринку і вести з ними конкурентоспроможну боротьбу за рахунок невисокої вартості впровадження та підтримки, а також потужної функціональності. Видимими відмінностями від конкуруючих компаній є: інтерпретування подій в зрозумілий вид, тегування та вагові показники, що дає більш зручний і швидкий спосіб аналізувати інформацію, що надходить. Також варто відзначити безлімітне кількість джерел інформації, що укупі з компактним сховищем дає можливість будувати оптимізовані запити на будь-якій глибині сховища.

2.1 Системи SIEM

SIEM (Security information and event management) у комп'ютерній безпеці є програмними продуктами, які об'єднують управління інформаційною безпекою SIM (англ. Security information management) та управління подіями безпеки SEM (англ. Security event management). Технологія SIEM забезпечує аналіз в реальному часі подій (тривог) безпеки, отриманих від мережевих пристроїв і додатків. SIEM представлено додатками, приладами або послугами, і використовується також для журналювання даних і генерації звітів в цілях сумісності з іншими бізнес-даними.

Зі зростаючим обсягом інформації яка обробляється і передається між різними інформаційними системами (ІС), організації та окремі користувачі все більше залежать від безперервності і коректності виконання даних процесів. Для реагування на загрози національній безпеці в ІС необхідно мати інструменти, що дозволяють аналізувати в реальному часі події, що відбуваються, число яких тільки зростає. Одним з варіантів розв'язання проблеми є використання SIEM-систем. Основний принцип системи SIEM полягає в тому, що дані про безпеку інформаційної системи збираються з різних джерел, і результат їх обробки надається в єдиному інтерфейсі, доступному для аналітиків безпеки, що полегшує вивчення характерних

особливостей, відповідних інцидентів безпеки. SIEM являє собою об'єднання систем управління інформаційною безпекою (SIM) і управління подіями безпеки (SEM) в єдину систему управління безпекою. Сегмент SIM, в основному, відповідає за аналіз історичних даних, намагаючись поліпшити довгострокову ефективність системи і оптимізувати зберігання історичних даних. Сегмент SEM, навпаки, робить акцент на вивантаженні з наявних даних певного обсягу інформації, за допомогою якого можуть бути негайно виявлені інциденти безпеки. У міру зростання потреб в додаткових можливостях безперервно розширюється і доповнюється функціональність даної категорії продуктів.

Однією з головних цілей використання SIEM-систем є підвищення рівня інформаційної безпеки в наявній архітектурі за рахунок забезпечення можливості маніпулювати інформацією про безпечність та здійснювати попереджувальне управління інцидентами і подіями безпеки в близькому до реального часу режимі.

Випереджаюче управління інцидентами і подіями безпеки полягає в прийнятті рішень ще до того, як ситуація стане критичною. Таке управління може здійснюватися з використанням автоматичних механізмів, які прогнозують майбутні події на основі історичних даних, а також автоматичного підстроювання параметрів моніторингу подій до конкретного стану системи.

SIEM представлено додатками, приладами або послугами, і використовується також для журналирования даних і генерації звітів з метою сумісності з іншими бізнес-даними.

Поняття управління подіями інформаційної безпеки (SIEM), введене Марком Ніколетта і Амріта Вільямсом з компанії Gartner в 2005 р, описує функціональність збору, аналізу та подання інформації від мережевих пристроїв і пристроїв безпеки, додатків ідентифікації (управління обліковими даними) і управління доступом, інструментів підтримки політики безпеки і відстеження вразливостей, операційних систем, баз даних і журналів

додатків, а також відомостей про зовнішні загрози. Основна увага приділяється управлінню привілеями користувачів і служб, службами каталогів і іншим змінам конфігурації, а також забезпечення аудиту та огляду журналів, реакцій на інциденти.

Деякі функції, зазвичай властиві SIEM:

– Завдання параметрів для реагування на важливі події;

– Запис логів і створення звітів, які будуть спрощувати аудит;

– Перегляд детальних даних.

Виходить, що SIEM збирає всі створені логи і статистику та зберігає їх в єдиному сховищі. Розмір сховища на пряму залежить від потреб конкретної системи. Серед лідерів ринку SEIM систем, можна виділити лише: McAfee Enterprise Security Manager, IBM QRadar SIEM, HP ArcSight.

Джерела даних для SIEM систем:

– Журнали подій. Які записуються тонкими і товстими клієнтами і контролюють права доступу;

– Антивіруси. Такий тип рішень, повідомляє про знаходження шкідливого програмного забезпечення або коду;

– DLP (Data Loss Prevention). Такі системи, контролюють і не допускають несанкціоноване переміщення інформації за межі мережі;

– Системи контролю доступу. Служать для отримання доступу до інформаційного потоку;

– IDS / IPS. Такі системи, передають інформацію про зміну прав доступу або мережевих атаках;

– Міжмережеві екрани. Такі рішення, передають інформацію про наявних шкідливий програмному забезпеченні і інциденти безпеки;

– Мережеве обладнання. Контролює призначений для користувача доступ до різних інфопотокам і зчитує трафік;

– Веб-фільтр. Дане доповнення, контролює доступ до шкідливих сайтів.

Деякі приклади індивідуальних правил для сповіщення за наявності певних подій включать правила аутентифікації користувача, визначення атак і вторгнень. Пороги реагування налаштовуються на утворення оповіщень небезпеки відповідно до кількості подій, що спостерігаються (таблиця 2.1).

Таблиця 2.1 - Приклади оповіщень

Правило	Мета	Тригер	Подія
Повторювана атака на логування	Вчасне попередження про атаки повного перебору, вгадування паролю та неправильної конфігурації застосунків.	Оповіщення при 3 і більше невдалих спробах залогінитись на хост протягом 1 хвилини.	Active Directory, Syslog (хости Unix Hosts, комутатори, марш рутизатори, VPN), RADIUS, TACACS, Monitored Applications.
Повторювана атака на мережевий екран	Вчасне попередження про сканування, розповсюдження хробаків, тощо.	Оповіщення при 15 і більше відмов мережевого екрану одній IP-адресі за хвилину.	Мережеві екрани, комутатори та маршрутизатори.
Повторювана мережева атака IPS	Вчасне попередження про сканування, розповсюдження хробаків, тощо.	Оповіщення при 7 і більше оповіщеннях від IDS від однієї IP-адреси за хвилину.	Пристрої виявлення та запобігання мережевого вторгнення
Повторювана атака на хост IPS	Виявлення хостів, які можуть бути інфіковані або скомпрометовані (їх поведінка вказує на те, що вони інфіковані)	Оповіщення при 3 і більше оповіщеннях від однієї IP-адреси за 10 хвилин.	Оповіщення від HIPS (Host Intrusion Prevention System)
Виявлення/видалення вірусів	Оповіщення коли вірус, шпигунське ПЗ або інше шкідливе ПЗ знайдено на хості	Попередження, коли один хост бачить ідентифікований шматок зловмисного ПЗ	Антивіруси, HIPS, Детектори аномальної поведінки в мережі/системі

Продовження таблиці 2.1

Виявлено вірус або шпигунське ПЗ, проте не вдалось його видалити	Попередження коли >1 години пройшло відтоді, як шкідливе ПЗ було виявлено, проте повідомлення про успішне видалення відсутнє	Попередження, коли один хост не зможе автоматично очистити шкідливе ПЗ протягом 1 години після його виявлення	Джерела подій: Firewall, NIPS, Антивірус, HIPS, Події не вдалого залогінювання

Отже, SIEM - це складна комплексна система, що дозволяє отримувати своєчасну і повну інформацію про стан IT-інфраструктури підприємства. SIEM-системи є досить непростими і дорогими інструментами управління електронними журналами. Складний процес впровадження і вимога до безперервного забезпечення збору подій і управління правилами кореляції вимагає наявність в штаті компанії кваліфікованих співробітників або залучення фахівців зі сторони інтегратора. Установка SIEM-системи без належного контролю і управління призведе до невиправданої витрати бюджету.

2.2 Система управління подіями інформаційної безпеки - HP ArcSight

Програмно-апаратне забезпечення HP ArcSight - це лінійка продуктів компанії Hewlett Packard, що лідирують у сфері моніторингу та контролю подій інформаційної безпеки. Рішення HP ArcSight здійснюють збір, обробку, зіставлення і реагування на такі події, надаючи всеосяжні функції масштабованості, захисту та відмовостійкості. Системи HP ArcSight дозволяє щохвилини обробляти сотні тисяч подій інформаційної безпеки, щоб автоматизувати рішення щодо забезпечення постійної ІБ в організації. Результати аналізу в режимі реального часу надаються адміністраторам безпеки в зручному вигляді для прийняття рішень з реагування на інциденти безпеки.

Технологія функціонування ArcSight передбачає поділ процесу обробки подій безпеки на п'ять основних етапів: фільтрація, нормалізація, агрегування, кореляція і візуалізація. В процесі фільтрації система видаляє події, які не мають прямого відношення до інцидентів інформаційної безпеки. На етапі нормалізації події приводяться до єдиного формату повідомлень ArcSight. Агрегування дозволяє видалити повторювані події, що описують один і той же інцидент. Ця процедура дозволяє значно скоротити обсяг інформації, яка зберігається і обробляється в системі моніторингу. Сформовані повідомлення потім обробляються, використовуючи механізми кореляції, засновані на статистичних методах, а також правила вбудованої експертної системи. І нарешті, ArcSight видає отримані результати на централізовану консоль, що працює в режимі реального часу.

ArcSight дозволяє адміністраторам безпеки сфокусуватися на реальні загрози, забезпечуючи їх засобами, що дозволяють оперативно реагувати на загрози безпеці мережі.

Інформаційні ресурси інтегруються в систему моніторингу в якості джерел повідомлень про події інформаційної безпеки за допомогою так званих конекторів (агентів).

Для візуалізації результатів роботи системи використовується консоль адміністратора, яка в реальному часі дозволяє проводити поділ подій за категоріями, кореляцію подій як по ресурсах, так і по зловмисникам, а також здійснювати детальний аналіз. За допомогою карти порушень безпеки можна отримати уявлення про відхилення в параметрах безпеки. Крім того, консоль забезпечена інтуїтивно зрозумілим інструментальним інтерфейсом і надає неперевершені можливості для підготовки табличних і графічних звітів про безпеку.

ArcSight дозволяє здійснювати моніторинг усіх необхідних ресурсів в режимі реального часу, отримуючи інформацію як на рівні засобів захисту, так і на рівні мережевих ресурсів, додатків і баз даних, що дозволяє

побудувати комплексну систему моніторингу та управління подіями інформаційної безпеки.

Ще однією особливістю системи ArcSight є можливість реалізації процесу управління інцидентами інформаційної безпеки строго відповідно до стандарту PCI DSS. [11]

2.3 Висновки до розділу 2

В наш час існує багато систем фіксації та управління подіями інформаційної безпеки. Вони являються програмними продуктами, що утворюють SIEM.

Однією з головних цілей використання SIEM-систем є підвищення рівня інформаційної безпеки в наявній архітектурі за рахунок забезпечення можливості маніпулювати інформацією про безпечність та здійснювати попереджувальне управління інцидентами і подіями безпеки в близькому до реального часу режимі.

Зазвичай вони представлені додатками, приладами, послугами, і використовуються для журналювання даних та генерації звітів з метою сумісності з іншими даними.

Основні функції, властиві SIEM:

– Завдання параметрів для реагування на важливі події;
– Запис логів і створення звітів, які будуть спрощувати аудит;
– Перегляд детальних даних.

3 ПІДХОДИ В ОЦІНЦІ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Існує багато способів оцінки інформаційного ризику.

Оцінка ризику - це процес, який використовується для присвоєння значень наслідків, ймовірності виникнення та рівня ризику. Вона включає в себе:

- оцінку ймовірності загроз і вразливостей, які можливі;
- розрахунок впливу, який може мати загроза на кожен актив;
- визначення кількісної або якісної вартості ризику.

На Рис. 3.1 представлені три способи, за допомогою яких можна проводити оцінку інформаційних ризиків:

- методи;
- управляючі документи;
- інструменти.

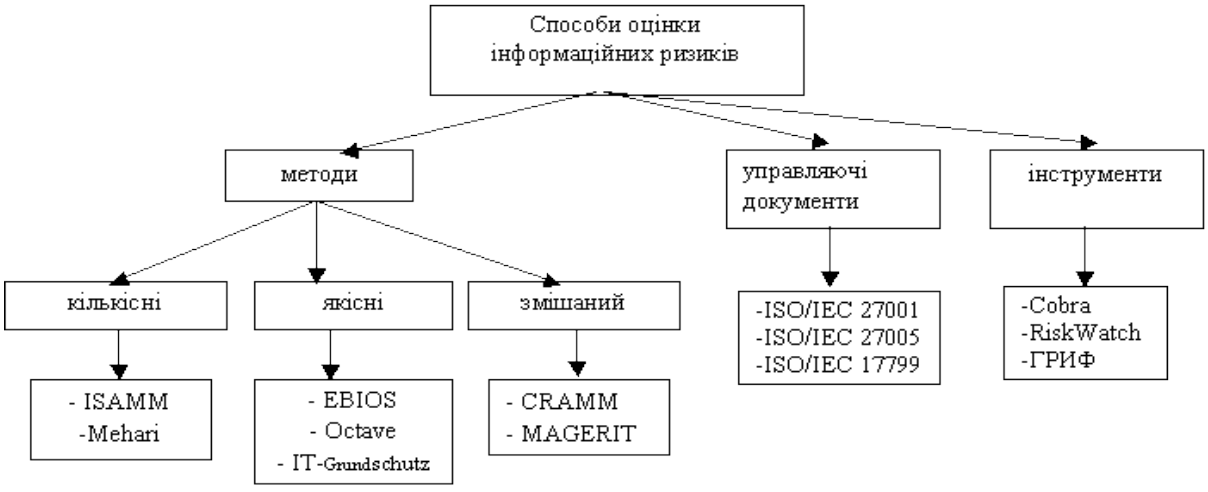

Рисунок 3.1 - Способи оцінки інформаційних ризиків.

3.1 Методи оцінки ризику

3.1.1 ISAMM

Виробник: Бельгія.

Опис: ISAMM була розроблена на основі Telindus. Це кількісний тип методології управління ризиками, де оцінюються ризики, виражаючи їх через щорічні очікувані збитків в грошових одиницях.

Щорічні очікувані збитки (ALE) = [ймовірність] X [середнє вплив].

ISAMM дозволяє показувати й моделювати зниження ризику для кожного поліпшеного контролю і порівнювати з його вартістю реалізації. Ефективність методу дозволяє виконувати обгрунтовану оцінку ризику в рамках, з мінімальними витратами часу і зусиль. Останньою еволюцією в методології ISAMM є уявлення активів. Це означає, що він може бути використаний для запуску оцінки ризиків щодо активів або згрупувати набір активів. Цей метод оцінки ризиків складається з трьох основних частин: огляду; оцінки; результат розрахунків та звітність.

Метод оцінки ризику: кількісний.

Наявність допоміжних програмних інструментів: немає, але має хорошу керівну документацію.

3.1.2 Mehari

Основним завданням MEHARI є надання методу оцінки і управління ризиками в сфері інформаційної безпеки, сумісного з вимогами ISO / IEC 27005, а також інструментів, необхідних для його впровадження [12]. Крім того, завдання MEHARI - надати індивідуальний аналіз ризикованих ситуацій (risk situations), описуваних сценаріями. Сценарій визначається в методології як опис всіх характеристик ризику, включаючи порушені активи, їх внутрішню уразливість і загрозу, що приводить до виникнення ризику [13].

Керівництво по процесу управління описує загальну технологію управління ризиками методології MEHARI і складові її етапи. В описі кожного етапу вказані його цілі, початкові умови, учасники етапу, підсумки етапу і процеси, що відбуваються на даному етапі. Вказівки щодо аналізу та класифікації ставок безпеки (security stakes) описує процес створення градації рівнів несправностей або порушень (malfunction value scale), а також класифікації активів компанії. Під ставкою безпеки в MEHARI маються на увазі наслідки, що представляють собою результат впливу інциденту безпеки на цілі організації. У керівництві з аналізу ризиків описано застосування бази знань MEHARI в процесі оцінки ризиків. База знань містить заготовки опитувальників для аудиту, списків загроз, активів, сценаріїв та інших елементів, які використовуються в методології, а також вбудовані функції розрахунку поточного значення рівня ризику на основі заповнених форм, представлених в базі.

Процес оцінки ризиків за методологією MEHARI складається з трьох етапів: упізнання ризику, аналізу ризику та оцінки [14].Впізнання ризиків полягає у визначенні сценаріїв, яким схильна організація.

Для кожного сценарію вказані:

– Основні порушені активи;

– Тип уразливості, що включає тип нанесеної шкоди (зникнення, зміна і ін.)

– критерії безпеки (конфіденційність, цілісність, доступність, а також ефективність (Для процесів управління по відношенню до виконання вимог замовників та нормативних

– документів));

– Тип загрози, що включає тип події, що приводить до загрози, його наслідки і що беруть участь осіб (actor) (в разі наявності людського фактора);

– Текстовий опис сценарію.

В ході аналізу для кожного сценарію визначаються ступінь впливу (impact) і ймовірність реалізації сценарію (likelihood), однак відбувається це не безпосередньо, а через проміжні характеристики: внутрішній вплив за відсутності захисних заходів (intrinsic impact), внутрішня ймовірність реалізації за відсутності захисних заходів (intrinsic likelihood), вплив захисних заходів на вищезгадані параметри. оцінка впливу та ймовірності за відсутності захисних заходів проводиться в зв'язку з тим, що вона простіше, а також тому, що проводять оцінку співробітники недооцінюють ризик, переоцінивши можливості впроваджених механізмів безпеки.

Захисні заходи, що відображаються на ймовірносты реалізації сценарію, поділяють на два типи - відлякуючі (dissuasive) і превентивні (preventive). Відлякуючі заходи спрямовані на учасників сценарію - зловмисників або рядових співробітників організацій. Превентивні включають в себе технічні заходи захисту і моніторинг механізмів, ефективність і міцність яких можна оцінити.

Захисні заходи, що впливають на вплив, діляться на обмежуючі (confinement) і пом'якшувальні (palliative). обмежучі заходи мають на увазі механізми, здатні стримати поширення наслідків порушення роботи одного компонента системи на інші. Пом'якшувальні заходи не стримують наслідки порушення безпосередньо, але призначені для зниження впливів на інші компоненти системи.

3.1.3 EBIOS

Виробник: Франція.

Опис: EBIOS являє собою повний набір посібників. Виробляються кращі практики, а також додатки документів, орієнтовані на кінцевих користувачів в різних контекстах. Цей метод широко використовується як в державному, так і приватному секторі. EBIOS формалізує підхід до оцінки ризику в області інформаційної безпеки систем. Метод враховує всі технічні

об'єкти (програмне і апаратне забезпечення, мережі) і нетехнічні об'єкти (організації, людські аспекти, фізична безпека).

Метод оцінки ризику: якісний.

Наявність допоміжних програмних інструментів: є.

3.2 Висновки до розділу 3

Розглянувши розділ я розглянув основні методи оцінки ризиків,а саме:

- EBIOS;
- Mehari;
- ISAMM.

Також з’ясував, що процес оцінки ризиків зазвичай складається з трьох етапів: упізнання ризику, аналізу ризику та оцінки [14]. Впізнання ризиків полягає у визначенні сценаріїв, яким схильна організація.

Для кожного сценарію вказані:

- Основні порушені активи;
- Тип уразливості, що включає тип нанесеної шкоди
- критерії безпеки (конфіденційність, цілісність, доступність, а також ефективність (Для процесів управління по відношенню до виконання вимог замовників та нормативних документів);
- тип загрози, що включає тип події, що приводить до загрози, його наслідки і що беруть участь осіб (actor) (в разі наявності людського фактора);
- текстовий опис сценарію.

4 ДОСЛІДЖЕННЯ МЕТОДІВ ОБРОБКИ РИЗИКІВ У СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

4.1 Зниження ризику

Зниження ризику означає, що підприємством вдаються до дій щодо зменшення ймовірності та / або впливу ризику, що, вимагає від керівництва компанії прийняття великої кількості оперативних рішень. Різновидами скорочення ризику можуть бути диверсифікація (розширення видів діяльності компанії), введення лімітів, формування резервів (на покриття збитків) і зменшення часу знаходження в небезпечних зонах (для виробничих циклів).

Застосування диверсифікації підприємствами малого бізнесу важко, що пояснюється особливостями бізнес-моделі підприємств такого масштабу - розширення видів діяльності потребують організації нових робочих місць, витрат у вигляді виплати заробітної плати, проте це не завжди можливо, оскільки ресурси компанії обмежені. Крім того, розширення видів діяльності вимагає достатньої компетенції та професійного досвіду від топ-менеджерів компанії, проте керівні пости малих підприємств можуть займати особи, які володіють недостатнім багажем знань і практичних навичок в галузі управління бізнесом (див. П. 4, табл. 1). Найбільш прийнятним для невеликих компаній може стати встановлення лімітів (наприклад, витрати матеріальних запасів, рівня кредитного навантаження підприємства, величини дебіторської заборгованості компанії і ін.). Це метод буде сприяти раціональному використанню та економії всіх видів ресурсів компанії, а також зниження рівня ризику. Освіта резервів також може бути використано організаціями подібних масштабів, оскільки методика їх створення була докладно описана в Росії і закріплена на законодавчому рівні. Скорочення часу знаходження в небезпечних зонах також можна застосувати підприємствами малого бізнесу, однак буде прямо залежати від специфіки фінансово-господарської діяльності компанії.

4.2 Прийняття ризику

Прийняття ризику означає, що керівництвом компанії не робиться ніяких дій для зниження ймовірності або впливу ризику через можливе отримання доходу (чим вище ризик, тим вище прибутковість вкладень) або через неминучість його настання. Прикладами прийняття ризику можуть бути: «самострахування» на випадок збитків і безпосереднє прийняття ризику, що відповідає рівню допустимого для компанії ризику. Підприємствами може застосовуватися утримання ризику, що включає в себе, крім прийняття ризику, також самострахування, т. Е. Створення резервів на покриття збитку. Сума утвореного при цьому резерву, як правило, дорівнює сумі, необхідної для повного покриття можливого збитку. Застосування зазначеного методу підприємствами малого бізнесу можливо, але може носити обмежений характер часто в силу відсутності достатнього обсягу ресурсів для створення резерву.

4.3 Запобігання ризику

Запобігання ризику передбачає припинення здійснення підприємством ризикової діяльності. Це метод може включати в себе закриття певного виду виробництва, відмова від виходу на нові ринки або прийняття рішення про продаж підрозділу і т.д. Щодо підприємств малого бізнесу застосування ухилення від ризику обмежена в силу того, що ризиковий вид фінансово-господарської діяльності може бути основним або, більш того, єдиним видом діяльності підприємства.

4.4 Передача ризику

Під передачею ризику мається на увазі перенесення або інший розподіл частини ризику, за рахунок чого досягається зменшення його величини.

Різновидами перерозподілу ризику є страхування, хеджування та передача певного виду діяльності сторонньої організації. Для малого підприємства такий спосіб, як передача певного виду діяльності, може означати додаткові витрати фінансових ресурсів компанії, з цієї причини він не матиме свого широкого практичного застосування. Хеджування як метод реагування на ризик може застосовуватися тільки тією частиною підприємств малого бізнесу, які стикаються з валютним ризиком і прагнуть уникнути фінансових втрат при несприятливому для компанії зміні курсу валют (зокрема, компаніями, що здійснюють експортно-імпортні операції). Застосування страхування не несе в собі будь-яких складнощів, однак вимагає додаткових витрат фінансових ресурсів. Невеликим компаніям слід застосовувати страхування у випадках, коли ймовірність настання події має вкрай низьку величину, а можливі негативні наслідки загрожують колосальними збитками (наприклад, страхування основних фондів компанії від пожежі).

4.5 Оцінка повернення інвестицій в інформаційну безпеку

Основною метою обробки ризику є вибір найбільш ефективних заходів, що забезпечують скорочення середньорічних втрат організації від інцидентів інформаційної безпеки при максимальному повернення інвестицій. Величина повернення інвестицій визначається як різниця між отриманою вигодою і вкладеними коштами. Як отриманої вигоди виступає оцінне значення скорочуваних середньорічних втрат, а в якості вкладених коштів - грошові кошти, прямо або побічно витрачені на механізми безпеки і забезпечують таке скорочення втрат.

[повернення інвестицій] = [зменшення середньорічних втрат] - [вартість захисних заходів]

Максимізація повернення інвестицій - основна економічна задача інформаційної безпеки. Бюджет на безпеку завжди обмежений, тому стоїть завдання вибору найбільш ефективних контрзаходів, тобто таких контрзаходів, які дають найбільший повернення інвестицій при найменших вкладеннях.

Для визначення того, наскільки ефективно захисні заходи скорочують втрати, використовується коефіцієнт повернення інвестицій (ROI) , який визначається як відношення величини повернення інвестицій до вартості реалізації контрзаходів, яка включає в себе витрати на їх планування, проектування, впровадження, експлуатацію, моніторинг та вдосконалення.

[Коефіцієнт повернення інвестицій (ROI)] = ([Зменшення середньорічних втрат] - [Вартість захисних заходів]) / [Вартість захисних заходів].

ROI показує, у скільки разів величина повернення інвестицій перевищує витрати на безпеку.

Графік зміни ROI в залежності від обсягу інвестицій в інформаційну безпеку показаний на рисунку 4.1

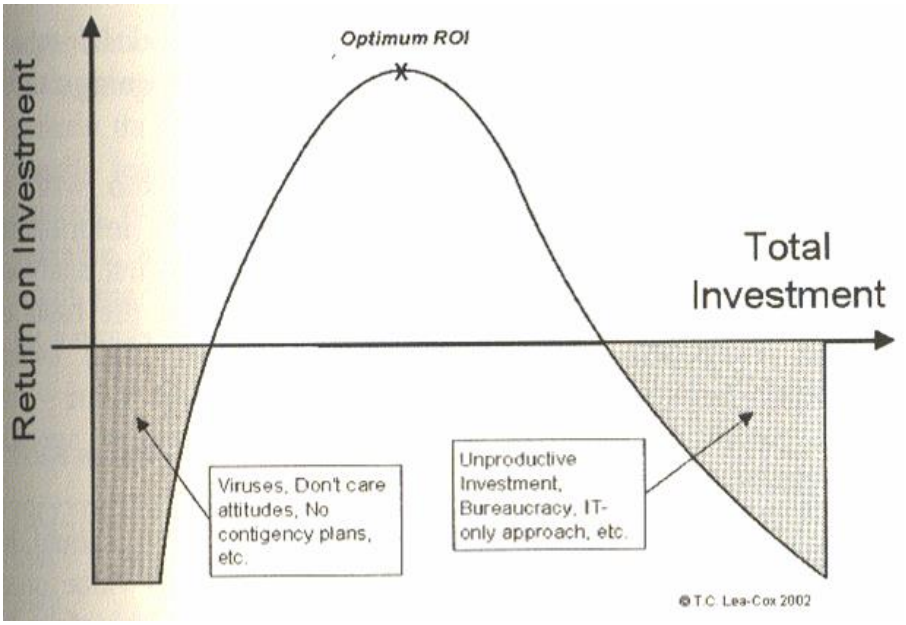

Рисунок 4.1 – Графік зміни ROI в залежності від обсягу інвестицій

Ми бачимо, що спочатку ROI перебуває в негативній області (області недофінансування). При збільшенні вкладень у безпеку, починаючи з певного рівня інвестицій ROI виходить в позитивну область (область оптимального фінансування) і поступово досягає свого максимального значення, а потім починає зменшуватися і знову входить в негативну область (область надлишкового фінансування).

Негативне повернення інвестицій (ROI <0) означає, що організація витрачає на безпеку більше, ніж отримує від цього вигод. У цьому випадку безпека є витратною статтею для організації, а захисні заходи обходяться дорожче отриманих переваг або тільки послаблюють реальний захист і призводять до зростання ризиків.

На схемі зафарбовані проблемні області з негативним поверненням інвестицій: область недофінансування і область надлишкового фінансування. У першому випадку гроші на безпеку виділяються в недостатньому обсязі за залишковим принципом. Заходи, що вживаються фрагментарні заходи не дають бажаного ефекту. Для цього випадку характерні проблеми з вірусами, відсутність планів безперервності бізнесу і легковажне ставлення персоналу до питань безпеки.

У другому випадку здійснюється надлишкове фінансування безпеки, але більша частина коштів витрачається даремно. Для цього випадку характерно процвітання бюрократії, надлишкова формалізація, придбання дорогого устаткування і / або програмного забезпечення без прийняття необхідних організаційних заходів.

При виборі способів обробки ризиків для кожного розглянутого механізму безпеки (способу обробки ризику) проводиться оцінка ROI. При цьому треба враховувати, що багато механізмів безпеки взаємопов'язані і у відриві від інших не дають необхідного ефекту, тобто не забезпечують бажаного повернення інвестицій. Так, політики безпеки або технічні засоби захисту не працюють без відповідного навчання і контрольних процедур. Тому при оцінці ROI найчастіше розглядається відразу група

взаємопов'язаних механізмів безпеки, які підтримують і доповнюють один одного, забезпечуючи максимальний ефект.

Припустимо, що за результатами оцінки ризиків ми отримали ALE ~ 1 млн. Дол. У цьому випадку щорічний повернення інвестицій в систему антивірусного захисту складе:

Δ ALE = 1000000 - 60000 = 940000 дол.

Коефіцієнт повернення інвестицій для системи антивірусного захисту дорівнюватиме:

ROI = 940000 / 60000 ~ 15,7.

Сукупність усіх цих чинників може давати абсолютно різні значення ROI. Крім цього, треба враховувати, що наші оцінки загроз, вразливостей і цінності активів є досить приблизними і допускають досить істотні похибки. Мінімальна і максимальна значення ALE можуть відрізнятися в кілька разів (але все ж не в десятки разів за умови, що оцінку ризиків проводять кваліфіковані експерти).

Тому значення ROI, що не перевищують 10, як правило, є не найкращими рішеннями для інформаційної безпеки (тому що з урахуванням можливої похибки оцінки реальний ROI при цьому може виявитися близький до 0). Ефективні механізми контролю як правило повинні мати більш високий коефіцієнт повернення інвестицій.

4.6 Висновки до розділу 4

По кожній загрозі необхідно прийняти рішення: прийняти ризик, знизити ризик або перенести ризик.

Прийняти ризик - значить усвідомити його, змиритися з його можливістю і продовжити діяти як раніше. Стосується загроз з малим збитком і малою вірогідністю виникнення.

Знизити ризик - значить увести додаткові заходи та засоби захисту, провести навчання персоналу і т д. Тобто провести навмисну роботу щодо зниження ризику. При цьому необхідно зробити кількісну оцінку ефективності додаткових заходів і засобів захисту. Всі витрати, які несе організація, починаючи від закупівлі засобів захисту до введення в експлуатацію (включаючи установку, настройку, навчання, супровід та ін.), Не повинні перевищувати розміру збитку від реалізації погрози.

Перенести ризик - значить перекласти наслідки від реалізації ризику на третю особу, наприклад за допомогою страхування.

В результаті кількісної оцінки ризиків повинні бути визначені:

– цінність активів в грошовому вираженні;

– повний список усіх загроз ІБ зі збитком від разового інциденту з кожної загрозу їх виникнення;

– частота реалізації кожної загрози;

– потенційний збиток від кожної загрози;

– рекомендовані заходи безпеки, контрзаходи, і дії по кожній із загроз.

ВИСНОВКИ

Стандарт ISO 27001 містить опис створення системи управління інформаційною безпекою організації. Реалізація багатьох положень цього стандарту залежить від специфіки організації. У сучасного бізнесу основною потребою є ідентифікування ризиків і управління ними. Технічні можливості постійно збільшуються, технічні засоби ускладнюються, вимоги стрімко ростуть. Стандарт ISO 27001 регламентує упорядкований підхід до вирішення проблем безпеки.

Поруч з елементами управління для комп'ютерів і мереж, стандарт приділяє значну увагу питанням розробки політики безпеки, роботі з персоналом (прийом на роботу, навчання, звільнення з роботи), забезпечення безперервності виробничого процесу, юридичним вимогам.

Вимоги даного стандарту мають загальний характер і можуть бути використані широким колом організацій - малих, середніх і великих - комерційних і промислових секторів ринку: фінансовому,страховому, в сфері телекомунікацій, комунальних послуг, в секторах роздрібної торгівлі і виробництва, різних галузях сервісу, транспортній сфері , органах влади та багатьох інших.

Стандарт ISO 27001 гармонізований зі стандартами систем менеджмент у якості ISO 9001 та ISO 14001 та базується на їх основних принципах. Більш того, обов'язкові процедури стандарту ISO 9001 потрібні і стандартом ISO 27001. Структура документації за вимогами ISO 27001 аналогічна структурі за вимогами ISO 9001. Велика частина документації, необхідна по ISO 27001, вже була розроблена, і могла використовуватися в рамках ISO 9001. Таким чином, якщо організація вже має систему менеджменту згідно з ISO 14001 або ISO 9001, то переважно забезпечується виконання вимоги стандарту ISO 27001 в рамках вже існуючих систем.

ПЕРЕЛІК ПОСИЛАНЬ

[1] irbis-nbuv.gov.ua;

[2] http://www.pdu-journal.kpu.zp.ua/archive;

[3] ISO/IEC27000URL:http://pqm-online.com/assets/files/pubs/translations/std/isomek-27000-2014.pdf;

[4] Общие сведения о стандартах серии ISO 27000. URL: http://www.iso27000.ru/;

[5] standarty/iso-27000-mezhdunarodnyestandarty-upravleniya-informacionnoibezopasnostyu-1/iso-27000-mezhdunarodnye-standarty-upravleniyainformacionnoi-bezopasnostyu.;

[6] ISO/IEC 27000. URL: http://pqm-online.com/;

[7] assets/files/pubs/translations/std/isomek-27000-2014.pdf.;

[8] ДСТУ ISO/IEC 27001-2015. URL: https://

[9] www.assistem.kiev.ua/doc/dstu_ISOIEC_27001_2015.pdf.;

[10] https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem;

[11] http://itsec.ru/articles2/Oborandteh/hp-arcsight--effektivnyy-instrument-dlya-monitoringa-sobytiy-ib;

[12] https://www.science-education.ru/ru/article/view?id=17991;

[13] K. Kavanagh, T. Bussa, G. Sadowski. Magic Quadrant for Security Information and Event Management. Gartner, 3 December 2018;

[14] CLUSIF MEHARI 2010 Overview. URL: http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-verview.pdf;

[15] CLUSIF MEHARI 2010 Fundamental concepts and functional specifications.URL:http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Principles-Specifications.pdf;

[16] CLUSIF MEHARI 2010 Risk analysis and treatment guide. URL: http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Risk-Analysis-and-Treatment-Guide.pdf;